Optical hiding with visual cryptography

Yishi Shi [1, 2*] and Xiubo Yang [1]

1. College of Material Science and Opto-Electronic Technology, University of Chinese Academy of Sciences, Beijing, 100049, People's Republic of China

2. Academy of Opto-Electronics, Chinese Academy of Sciences, Beijing 100094, People's Republic of China

*E-mail: optsys@gmail.com (Y. Shi)

Received Month X, XXXX; revised Month X, XXXX; accepted Month X, XXXX;
published Month X, XXXX

Abstract

Classical optical hiding methods are symmetric, being apt to realize but not secure. The security is improved in existing non-symmetric hiding techniques, yet all of them fails in convenient extractions, still not optically realized so far. Here, we propose an asymmetric optical hiding method based on visual cryptography, achieving the high security and the easy extraction at the same time. In the hiding process, we convert the secret information into a set of fabricated phase-keys, which are completely independent of each other, intensity-detected-proof, and image-covered, this complex hiding procedure leading to the high security. Correspondingly, during the extraction process, the covered phase-keys are illuminated with laser beams and then incoherent superposed to extract the hidden information directly by human visual system, without complicated optical implementations and any additional computation, resulting in the convenience of extracting. Optical experiments verify that both the high security and the easy extraction are obtainable in the visual-cryptography-based optical hiding.

Keywords: optical hiding, Fourier optics, visual cryptography, phase-only keys

1. Introduction

The inherent nature of optics offers many possibilities for information hiding applications [1-14]. Classical optical hiding techniques are symmetric, in which the extraction is the inverse process of the hiding. It implies that if the extraction is easy to perform, the corresponding hiding process is relatively less complex, thereby the security risk is increased [1-9]. Some non-symmetric methods have been proposed to alleviate the conflict between the security and the convenience. However, in these methods, the security is often improved, but the difficulty of extractions is not satisfactorily dropped, and in fact they are still not optically realized so far [10-13]. In this Letter, utilizing the asymmetry of visual cryptography [15-18], we propose a new optical hiding technique to attain the high security and the easy extraction at the same time, as demonstrated by optical experiments.

2. Theory

2.1 Hiding procedure of visual-cryptography-based optical hiding

Let us briefly describe how to conduct visual-cryptography-based optical hiding (VCOH). Figure 1 presents the hiding process of VCOH with three steps. Suppose "OK" is the information to be hidden. In Step 1, we employ the encoding principle of visual cryptography: the "OK" is visualized as a binary image after expanding the pixel-units and then is generated into a set of visual-keys, in which each pixel-unit at the same position is randomly chosen one by one based on the pixel expansion rule. This can be accomplished with a regular algorithm of visual cryptography [15]. If each pixel-unit is composed of a 2×2 array, two of generated visual-keys with mosaic like distributions are shown in Fig. 1. Note that, even in this case, which is one of the simplest examples of visual-cryptography-based encoding [15], still well presenting the core spirit of visual cryptography, these visual-keys are completely unrelated with each other. Thus, Step 1 makes VCOH be quite distinguished from the other optical hiding methods [13],

and provides a firm security basement that will be further examined later on. Then Step 2 is the phase hiding: according to the visual-keys' distributions, we calculate the phase-keys one by one with a phase retrieval algorithm [20], ensuring each obtained phase-key illuminated by a laser beam with a designed wavelength to project the intensity pattern of the counterpart visual-key. As the original visual-keys are usually random like distributed, they are liable to attract the attention of attackers. This step effectively reduces the possibility of being attacked, since the information of phase-only keys are directly undetectable with the intensity detectors such as CCD and naked eyes. Thus Step 2 enhances the security of VCOH once again. At last, Step 3 is the image hiding: using the fabrication techniques such as producing the diffractive optical elements, we fabricate the phase-keys as the real transparent plates, then cover them with printed images, such as Panda and Girl shown in Fig. 1. As these phase-keys are hidden in the intensity images with the concealment increased, the security of VCOH is ensured further.

After three steps above, the secret information "OK" is hidden in a group of the fabricated phase-keys, being completely-mutually-unrelated, intensity-detected-proof and images-covered. Consequently, the hiding process of VCOH is sufficiently complicated, leading to the high security for concealing purposes.

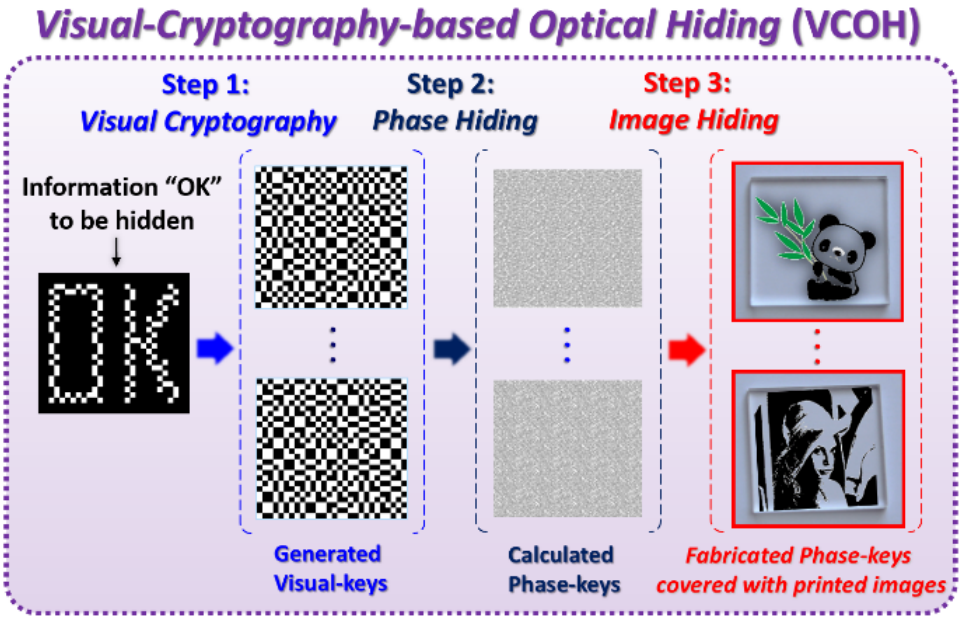

Fig.1 Optical hiding with visual cryptography: the hiding procedure.

2.2 Optical extraction of visual-cryptography-based optical hiding

Correspondingly, the extraction process of VCOH is shown as Fig. 2. Using the laser beams with designated wavelengths $\{\lambda_1, \lambda_2 \ldots \lambda_n\}$ to illuminate the set of fabricated phase-keys, we can recover the intensity patterns corresponding to the original visual-keys on a reflective surface. If we incoherently superpose these recovered visual-keys, we can extract the secret information "OK" directly by the human visual system without any additional computation [15]. It is due to the human visual system has the ability to perform the correlation computation quite well [19], which is the source of visual cryptography's asymmetry [15-18]. Note that, although the visual-keys needs to be recovered with coherent illumination, the superposing of the visual-keys only requires incoherent operation, being quite convenient for practice. In addition, we can receive the extracted "OK" in the near or the far field, as determined by the Fresnel or the Fourier transform used in the phase retrieval algorithm for phase-keys designs. As a result, since the incoherent superposition is easy to align and the recognition only relies on the human vision, the extraction is convenient even for the users without any knowledge about optical hiding.

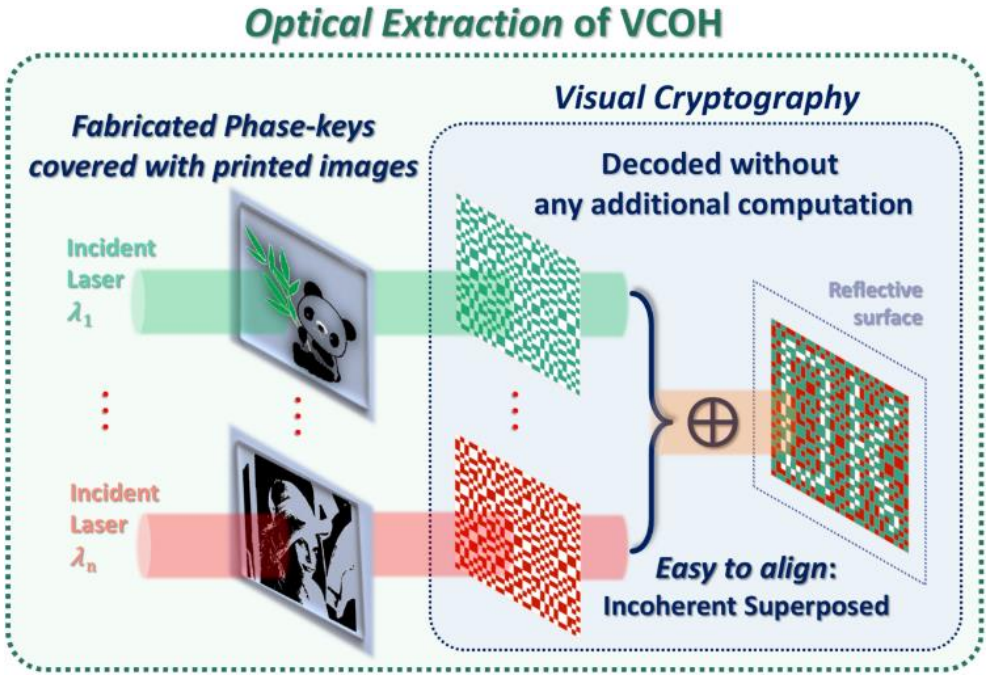

Fig.2 Optical hiding with visual cryptography: the optical extraction.

3. Experimental results

3.1 Experimental results for 3D object hiding

We have performed optical experiments to demonstrate VCOH. The hiding results and extraction results are all shown in Fig. 3. We still take "OK" as the information to be hidden. In the hiding process, with Step 1 described as above, "OK" is visualized as a binary image with pixel expansions shown as Fig. 3 (a) and then is encoded to a set of visual-keys. Here, as our primary aim is to verify the feasibility of VCOH but not to explore its potential ability, we choose the nearly the simplest encoding way of visual cryptography, obtaining that one set only consists of two visual-keys with 2×2 array pixel-units (a two out of two secret sharing solution, the case of (2, 2) [15]), shown as Fig. 3 (b) and (c). With Step 2 of the phase hiding, the visual-keys are correspondingly transformed to the phase-keys calculated with the phase retrieval algorithm, the grayscale forms of which are shown as Fig. 3 (d) and (e). For instance, it ensures the intensity of the phase-key$_1$'s Fourier transformation to be the distribution of visual-key$_1$. Then with Step 3 of the image hiding, the phase-keys are fabricated just as the diffractive optical elements with the help of a commercial company [21], with the size about 1.2 × 1.2 cm^2, and then they are covered with images Panda and Girl. They are printed on the transparent plastics then tied on the fabricated phase-keys, respectively, shown as Fig. 3 (f) and (g). At last, the "Panda" and the "Girl" are the hiding results.

Then we examine the optical extracted results of VCOH. When an authorized user collects the “Panda” and the “Girl” together, shown as Fig. 3(f) and (g), he can begin to extract the hidden information. If all of these fabricated phase-keys are illuminated by expanded laser beams with the designed wavelengths of λ_1 (532 nm) and λ_2 (632.8 nm), the output intensities projecting on a reflective surface are the recovered visual-keys shown as Fig. 3(k) and (i), respectively. Superposing the optically recovered visual-keys, the user can directly identify the extracted "OK" shown as Fig. 3 (m) by his own

vision. Because the human visual system has the ability to accomplish the correlation calculation with the high accuracy and efficiency, the user easily recognizes the yellow-black-outlined “OK” as the extraction distinguished from the green-and-red background, as shown in Fig. 3 (m), quite similar to the visualized “OK” shown as Fig. 3 (a). In this way, if the incident wavelengths are both 632.8 nm, the recovered visual-keys are shown as Fig. 3(h) and (i), respectively, and the optically extraction is presented as Fig. 4 (j). Again, the extracted “OK” is recognizable, similar to the case of Fig. 3(m). Thus, the easy extraction of VCOH is verified experimentally.

For the optical extractions in VCOH, some notes need to point out. First, the extraction of VCOH is easy to achieve optically. It only requires the incoherent superposition in optical extractions, without any complicated optical implementations, such as the interferometric ones [3, 7] or the coherent-cascaded ones [10-13]. This is owing to the asymmetry introduced by visual cryptography. As the decoding of visual cryptography needs no additional computations but human recognitions, the extraction is obtainable just by stacking the recovered visual-keys together. Hence, the extract process of VCOH is much easier to be realized optically than the coherent setups [11, 13]. In addition, as the fabricated phase-keys are essentially the optical diffractive elements, generally with a tolerance of the incident wavelength in some range, it allows the visual-keys recovered with varied wavelengths shown in Fig. 3(k) to (m), which also facilitates the extraction process.

Second, VCOH’s extracted quality is quite acceptable. It is due to the optical merits of fabricated phase-keys. On the one hand, the phase-keys mainly made up of diffractive optical elements are robust to various disturbances. For instance, the phase-keys are covered with the printed images, increasing the concealment for VCOH but actually causing the noises of the optically recovered visual-keys, the distributions of which still fit well with original visual-keys at a high signal-noise ratio. The further test

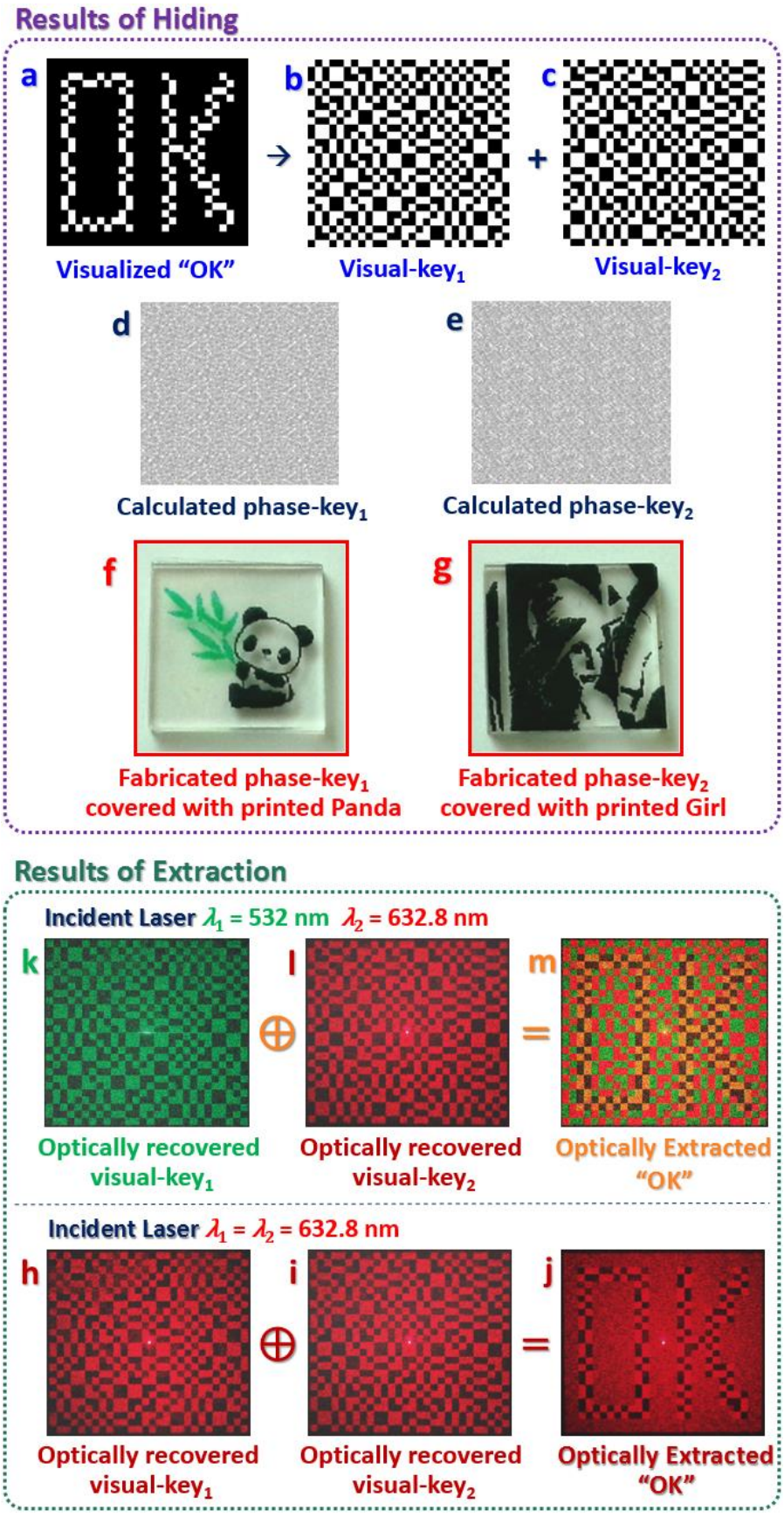

Fig.3 Optical experimental results of VCOH: (a) to (f) and (l) to (j) are the results of hiding and extraction, respectively.

results will be given in detail later on. On the other hand, the incoherent superposition depresses the speckled noises in the recovered visual-keys. Due to the coherent illumination on the phase-keys, the optically recovered visual-keys inherently have the random-like speckled noises. Fortunately, this problem is alleviated by the incoherent superposition. Note that the "or" logical operation is performed in the decoding of pure visual cryptography, while the "and" logical operation is in the extraction of VCOH. Thus the background of the extracted "OK" in VCOH is lighted as shown in Fig. 3(j) but not just black in Fig. 3 (a), for a background's red pixel only comes from one of visual-keys'. Different from the background, the red pixels of the core part of "OK" is superposed by all of recovered visual-keys. Although each red pixel of recovered visual-keys carries the random-like speckled noises, the incoherent superposition of these noises depresses the randomness mutually with direct additions, giving a smoother and more stable distribution of the core part of "OK". Its enhanced contrast results the optical extracted "OK" is more recognizable for the human vision, presented as Fig. 3 (j). Further, as shown in Fig. 3 (m), in the case of extractions with diverse wavelengths, the speckled noises' affection is decreased by the color distinguishing. Therefore, the extraction quality of VCOH is optically demonstrated.

4. Security analysis

Then, let us analyze the security of VCOH. Its security is ensured by both the optical aspect and the visual-cryptography aspect. As presented above, in VCOH, the information is hidden as a set of fabricated phase-keys, which are printed-images-covered, intensity-detected-proof, and totally-mutual-unrelated. Certainly, the former two factors are the optical aspect of VCOH's security, while the latter one is the visual-cryptography aspect.

4.1 Security of the optical aspect

On the one hand, we examine the optical aspect. The covered printed images offer the basic but effective concealment for VCOH. They make the fabricated phase-keys quite similar to the usually used

printing productions, being able to escape from the attackers' routine detections. More importantly, the phase-keys are intensity-detected-proof, which can satisfy the hiding requirement quite well. These keys are able to pass the normal ways of detections, for the structural information of them cannot be revealed directly by the intensity detectors such as CCD or CMOS cameras except using complicated interferometric detection. In addition, the phase-keys, which can be designed to only respond to special wavelengths such as terahertz-wave [14] instead of the visible light here, would strengthen the security further.

4.2 Security of the visual-cryptography aspect

On the other hand, we discuss the visual-cryptography aspect. First of all, we review the procedure of encoding and decoding "OK" by visual cryptography. If n visual-keys are generated as encoding results and k of them allow the successful decoding of "OK", it is the case of (k, n) [15]. Here, k and n are both set to two, being the simplest case. In the encoding procedure, "OK" is transformed to a binary image that is then pixel-expanded further, as shown in Fig. 4 (a). We employ three pairs of pixel-units presented in Fig. 4 (b) for the pixel expansion if pixel-units are 2×2 array in size. Figure 4 (c) takes the first pair of pixel-units as an example to show the rule of the pixel expansion. To gain a black expanded-pixel, two different pixel-units in the same pair require to stack together, while the same two pixel-units are superposed to be a white expanded-pixel. In this way, according to the image-transformed "OK", we randomly choose the pixel-units pair to generate each expanded pixel separately, and obtain two visual-keys shown as Fig. 4(d) as the encoding results. Correspondingly, in the decoding procedure, two correct visual-keys are stacked together to recover the pixel-expansion "OK", which is able to be identified and revealed directly by the human visual system. Thus, the pixel expansion with randomly chosen pixel-units makes the correlation recognition in the decoding become necessary. This recognition is much

easier and more accurate for the human visual system than the machine system. It is the core spirit of visual cryptography, and its introduced security will be analyzed further as below.

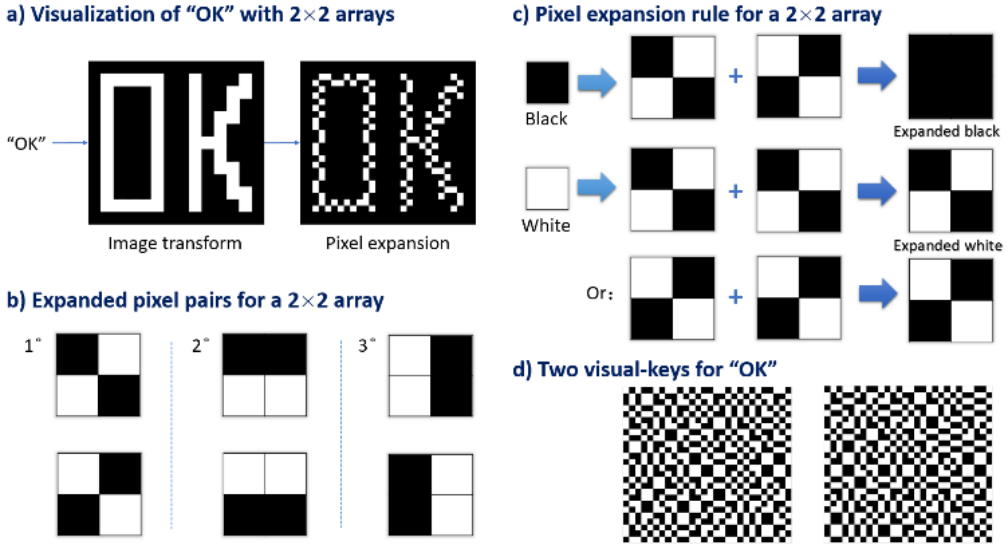

Fig. 4. Asymmetry: security introduced by visual cryptography.

Now we focus on the security of VCOH introduced by visual cryptography. To test the security of the above case, we try our best to breach this cryptosystem. Assume that we already obtain one of visual-keys, and need to deduce the other one correctly. Since each pixel-unit is randomly chosen one by one in the encoding, the pixel-units in one of visual-keys are independent of each other. Based on the rule shown in Fig. 4 (c), when a pixel-unit in one visual-key is defined, the other visual-key's pixel-unit in the same position should be itself or the one in its pair. Thus, there is a half chance to correctly deduce the corresponding pixel-unit of the other visual key. In the "OK" case, one visual-key being formed with 13×14 pixel-units, the other visual-key has a chance of $(1/2)^{(13\times14)}$($=1.63\times10^{-55}$) to be correctly deduced. That is, we need to find the correct visual-key in the key-space with $1/(1/2)^{(13*14)}$ ($=6.13\times10^{55}$) possible keys. The key-space seems not a very big with a rising hope for the correct deduction. Unfortunately, it is not true. When we generate a new guessed visual-key, we need to superpose it with the known one to gain the decoded information. As the key-space is not small even in the case of "OK" with 13×14

pixel-units, the computer requires to be employed for the recognition of decoded information. In fact, although the recognition rate of the machine visual system is quite close to 100% in one-time recognition, the computer cannot reach 100%. Suppose that the once recognition rate is 99.9999%. If 10^8 recognitions are done, the total recognition rate is 3.72×10^{-44} (=99.9999% to the power of 10^8), while it drops to 5.07×10^{-435} (=99.9999% to the power of 10^9) after 10^9 recognitions. According to this trend, in the case of 6.13×10^{55} guessed visual-keys requiring to be recognized, the total recognition rate will fall into zero in fact. It reveals that even for the simplest case of visual cryptography, it is quite hard to deduce one visual-key from the other. That is, the two visual-keys are completely unrelated. Further, neither visual-key allows the secret information to leak out. Therefore, visual cryptography provides a firm security basement for VCOH.

5. Robustness analysis

The robustness of VCOH has also been testified. Considering that various distortions in practice to VCOH can be summarize as the phase noises to the fabricated-covered phase-keys, in the test we add the phase noises directly to the phase-keys. For the simplicity of quantity analysis, we still take the scheme of two phase-keys, and not fabricate them but instead, upload their phase distributions to two spatial light modulators (SLMs), respectively. The random noises are also loaded and added to SLMs directly. This time, the secret information is the digital numbers "70". We use the correlation coefficient (Co) between the extracted image without and with the phase noise to evaluate the extraction quality. The value of Co is in the range of [0, 1], and the minimum and the maximum value means the poorest and the best extraction quality, respectively [22, 23]. Optical experiments present that the Co slowly drops down with the phase noise increasing shown in Fig. 5. Especially, when one time of random noise is added, the extracted "70" is still recognizable. Even the noise achieves 1.4 times, some information of "70" can be recognized. Until 1.6 times noise is added, the extraction totally turns to a random-like distribution. As

the phase noise can well stands for various distortions to fabricated-covered phase-keys, these experimental results are able to prove the strong robustness of VCOH.

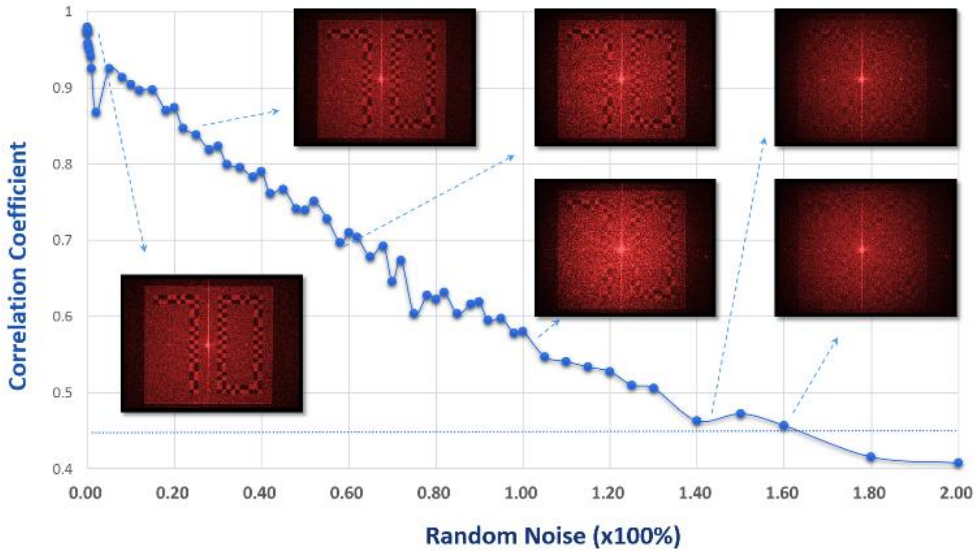

Fig. 5 Robustness analysis of optical hiding with visual cryptography.

6. Conclusions

In summary, we combine optical hiding with visual cryptography and verify it optically. In the hiding process, the secret information is hidden into a group of fabricated phase-keys, being mutually-unrelated, intensity-detected-proof and images-covered, resulting the high security of concealments. Due to the asymmetry of visual cryptography, the extraction process does not require complicated optical implementations and any additional computations, being convenient even for the users without any knowledge about optical hiding. Also, VCOH is verified robust to noises. In the future, the proposed VCOH could be developed into a class of optical hiding techniques with both the high security and the practicable value.

Acknowledgments

National Natural Science Foundation of China (61575197); Fusion Foundation of Research and Education of CAS; Youth Innovation Promotion Association CAS. We are very grateful to Prof. Yongliang Yu for his invaluable suggestions and thank Dr. Tuo Li, Mr. Yong Luo and Miss Wenhui Xu for their important supports to this paper.

References

1. J. Rosen and B. Javidi 2001 Hidden images in halftone pictures *Appl. Opt.* **40** 3346-3353
2. S. Kishk and B. Javidi 2002 Information hiding technique with double phase encoding *Appl. Opt.* **41** 5462-5470
3. S. Kishk and B. Javidi 2003 Watermarking of three-dimensional objects by digital holography *Opt. Lett.* **28** 167-169
4. H. Kim and Y. H. Lee 2005 Optimal watermarking of digital hologram of 3-D object *Opt. Express* **13** 2881-2886
5. Y. Shi, G. Situ and J. Zhang 2008 Multiple-image hiding by information prechoosing *Opt. Lett.* **33** 542-544
6. H. Hamam 2010 Digital holography-based steganography *Opt. Lett.* **35** 4175-4177
7. J. Li, J. Li, L. Shen, Y. Pan and R. Li 2014 Optical image encryption and hiding based on a modified Mach-Zehnder interferometer *Opt. Express* **22** 4849-4860
8. J. Zhang, Z. Wang, T. Li, A. Pan, Y. Wang and Y. Shi 2016 3D object hiding using three-dimensional ptychography *J. Opt.* **18** 095701
9. W. Xu, H. Xu, Y. Luo, T. Li and Y. Shi 2016 Optical watermarking based on single-shot-ptychography encoding *Opt. Express* **24** 27922-27936
10. Y. Shi, G. Situ and J. Zhang 2006 Optical image hiding in the Fresnel domain *J. Opt. A: Pure Appl. Opt.* **8** 569
11. Y. Shi, G. Situ and J. Zhang 2007 Multiple-image hiding in the Fresnel domain *Opt. Lett.* **32** 1914-1916
12. X. Wang, W. Chen and X. Chen 2014 Fractional Fourier domain optical image hiding using phase retrieval algorithm based on iterative nonlinear double random phase encoding *Opt. Express* **22** 22981-22995
13. X. Wang, W. Chen, S. Mei and X. Chen 2015 Optically secured information retrieval using two authenticated phase-only masks *Scientific Reports* **5** 15668
14. A. Chanana, A. Paulsen, S. Guruswamy and A. Nahata 2016 Hiding multi-level multi-color images in terahertz metasurfaces *Optica* **3** 1466-1470
15. M. Naor and A. Shamir 1995 Visual cryptography *Advances in cryptology. Eurocrypt '94 Proceeding LNCS* **950** 1-12
16. Ateniese, G., C. Blundo, A. De Santis and D. R. Stinson 2001 Extended capabilities for visual cryptography *Theoretical Computer Science* **250** 143-161
17. S. J. Shyu, S. Y. Huang, Y. K. Lee, R. Z. Wang and K. Chen 2007 Sharing multiple secrets in visual cryptography *Pattern Recogn.* **40** 3633-3651
18. L. Glass 1969 Moiré Effect from Random Dots *Nature* **223** 578-579
19. J. R. Fienup 1982 Phase Retrieval Algorithms: A Comparison *Appl. Opt.* **21** 2758-2769
20. http://en.homolaser.com
21. Y. Shi, T. Li, Y. Wang, Q. Gao, S. Zhang and H. Li 2013 Optical image encryption via ptychography *Opt. Lett.* **38** 1425-1427
22. T. Li and Y. Shi 2015 Security risk of diffractive-imaging-based optical cryptosystem *Opt. Express* **23** 21384-21391